Before the Federal Communications Commission
Washington DC 20554

In the Matter of

Amendment of Part 97 of the Commission's
Amateur Radio Service Rules to Reduce
Interference and Add Transparency to Digital Data
Communications

RM-11831

Reply Comments to Ted Rappaport, N9NB

This is a reply to comments filed by Ted Rappaport, N9NB.

I need to stress that, as an experimenter, I am less concerned with the existing Pactor/ Winlink network (which I don't use) than with the serious effect that these proposed restrictions will have on the future development of digital communications on the amateur bands. I am

especially concerned with those who want to teach themselves the principles of digital communications — and possibly advance the state of the art — by experimenting with their own designs on the air. This is directly in keeping with the Basis and Purpose of the Amateur Service.

Rappaport and I now agree on proprietary decoders

I am gratified that Rappaport would allow the proprietary voice codecs used by amateur digital voice networks such as DMR, D*Star and Fusion because of the availability of hardware codecs that can be used to monitor digital voice transmissions. While I strongly share Rappaport's concern about proprietary (i.e., undocumented) air interfaces on the amateur bands, neither of us want the serious unintended consequences of legally banning them. I personally prefer to make my case against proprietary technology not by legal force, but by building superior open alternatives and persuading amateurs to use them. I invite Prof Rappaport, an expert in the field of digital radio communications, to do the same.

Since the same principle would have to apply to Pactor/Winlink, a proprietary decoder should meet the requirement — as much as I would personally like to see an open-source version.

Rappaport continues to use the inflammatory and misleading term "effectively encrypted"

As we all know, *true* encryption is and should remain prohibited on the amateur bands. For this reason, "encryption" is a loaded word among radio amateurs, and I object to Rappaport repeatedly pushing this emotional button with the misleading term "*effectively* encrypted". He uses this term because he knows that the communications at issue do not meet the formal

definition of encryption. That rule has always rested on *intent*: if the *intent* of some technique is to obscure the meaning of a communication, it falls under the prohibition; if the *intent* is merely to facilitate communications it is allowed *even if* it has the effect of making the communication more difficult (for some parties) to monitor. [1] This is the correct rule, and it should remain so.

As I explained in detail in my comments, *anything* one might do to facilitate communications and use the spectrum more efficiently *necessarily* makes that communication more difficult for (some) third parties to monitor. That's just math and physics. On page 12 of his comments, Rappaport accepts this fact:

> "Mr. Karn describes how more efficient communications inherently become harder to decode, which is generally true…."

This one concession fatally undercuts his entire argument! He continues:

> "…but FCC Part 97.113 makes clear that efficiency cannot be used as an excuse to obscure the transmitted signal for meaning"

Actually, the rules *do not* say that! They only prohibit "messages encoded for the purpose of obscuring their meaning". Period. This couldn't be clearer. If the *purpose* of the encoding is to facilitate communication, it is allowed even if it has the side effect (as it often necessarily will)

---

[1] In this age of weak computer and network security, it would be difficult to demonstrate a serious intent to obscure a communication without the explicit use of an encryption algorithm (e.g., AES) with a properly designed key management scheme. No one has alleged that Winlink/Pactor do this.

of “obscuring their meaning” to other stations. That remains true even if others mistakenly believe that the system is somehow secure.[2]

ARQ is a generic, widely used technique not limited to Pactor/ Winlink

Rappaport is justly regarded as an expert in the physical layer, i.e., propagation, modulation and coding, but he seems to lack basic knowledge of higher layer protocols in digital communications. Apparently unfamiliar with standard practice, Rappaport characterizes ARQ as a nefarious scheme intended to obscure communications. Nothing could be further from the truth. ARQ (Automatic Request Repeat) has been a standard, generic feature of many communication protocols above the physical layer for many decades, e.g., the AX.25 Amateur Packet Radio link level protocol.[3] It is used in 802.11 (WiFi) wireless LANs.[4] And it is in the Internet’s Transmission Control Protocol (TCP), which I implemented for amateur packet radio in 1986. He describes ARQ as a “code” when it is actually a simple procedure. Far from being suited only to wireline communications, ARQ is *essential* to reliable communications. Contrary to Rappaport’s claim, forward error correction (FEC) *cannot* guarantee reliability; it is merely an optional performance enhancement (though a very important one on radio channels).[5] [6]

---

[2] Security experts repeatedly stress (and demonstrate) the folly of “security through obscurity”.

[3] Amateur Radio Link Layer Protocol AX.25 https://www.tapr.org/pdf/AX25.2.2.pdf

[4] WiFi doesn’t rely on ARQ for security. It uses explicit encryption described in a separate standard, IEEE 802.1x.

[5] End to End Arguments in System Design, J.H. Saltzer, D.P. Reed, D.D. Clark; MIT Laboratory for Computer Science, 1984. http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf This paper is justly considered a classic in network design.

[6] The Internet Engineering Task Force (IETF) has long struggled with the “reliable multicast” problem, where one transmitter must be reliably received by many receivers. It has suggested a variety of approaches that combine FEC and/or individual acknowledgements (i.e., modified ARQ) but the general problem for large numbers of receivers remains unsolved and is probably unsolvable. In practice, multicast applications must be designed to tolerate data loss.

> "Mr. Karn and others should know that the commercial wireless industry uses published FEC codes instead of ARQ codes in broadcast channels where other mobile users need to listen in on the channel. Just like a broadcast mobile wireless (cellphone) system that undergoes fading, FEC can be used to provide HF amateur radio data stations with excellent anti-fading performance, excellent spectral efficiency, error-free communication, and complete data transparency to other users."

This is simply incorrect. The commercial wireless industry uses *both* FEC and ARQ in combination. [7] This is true for both commercial wireless services and for 802.11 (WiFi) wireless LANs. In addition, every Internet user also uses the ARQ built into the Transmission Control Protocol (TCP).

Indeed, WiFi clearly demonstrates the difficulty of passive channel monitoring with FEC alone. WiFi normally uses link-level acknowledgements (i.e., ARQ) to provide reliable delivery of "unicast" packets to specific receivers. It also provides a "multicast" facility where packets are transmitted without ARQ at a low data rate for all stations. In practice this works very poorly; the low data rate causes any significant amount of multicast traffic to saturate the channel, and the lack of ARQ results in a very high loss rate. The current workaround is "multicast to unicast conversion", where a separate copy of each multicast packet is transmitted to each receiver and acknowledged by that receiver. Because these transmissions occur at whatever data rate the receiver can handle, which is usually much faster than the base multicast data rate, overall efficiency is substantially improved as long as the number of receivers is not large. But again,

---

[7] I personally developed the first link layer protocol to carry Internet data over Qualcomm's CDMA digital cellular system. It used an ARQ scheme with negative acknowledgements.

this requires active participation by each receiver; reliable passive multicasting remains an unsolved problem.

Rappaport claims:

> "The ARSFI/Winlink methods that rely on ARQ and compression are most likely less spectrally efficient than if they used FEC (e.g. Viterbi decoding)."

This reveals a profound ignorance of how this system actually works. Once again, *both* ARQ and FEC are used. The Pactor modem uses strong FEC to improve the reliability of the physical layer, but FEC alone cannot guarantee reliability so ARQ is layered on top of the FEC to retransmit transmissions that the FEC is unable to decode. Countless other systems for both radio and wire use this well-proven hybrid. Many (e.g., WiFi) integrate the two features, e.g., by varying the FEC code rate in response to the ARQ retransmission rate. Some use ARQ to transmit additional FEC parity symbols that can be combined with previous transmissions that were undecodeable by themselves. This is often much more effective than simply retransmitting from scratch.

ARQ couldn't be simpler or easier to monitor. Each packet or frame of data is given a sequence number so that receivers can detect losses and request retransmissions. A monitoring station can just as easily examine the sequence number and discard any duplicates. It can detect losses, but as a passive listener it cannot request retransmissions.

Not only does Rappaport's suggestion that FEC be used instead of ARQ fly in the face of many decades of experience in protocol design, FEC could actually make his claimed problem worse! Without FEC, fading channels (like HF) require high link margins (i.e. excess transmitter power) to reduce the packet loss rate to an acceptable level. Even with ARQ, one wants to avoid the poor performance associated with excessive retransmissions of missing data. These excessive margins make the signal easier to overhear. But with FEC designed for a fading channel, power levels can be significantly reduced and link margins significantly tightened. These tighter margins can make it more difficult for third parties to monitor the signal when the link from the transmitter is even a little worse than the link from the transmitter to the intended recipient. It's a perfect example of the principle that *anything* one might do to use spectrum more efficiently can have the side effect of making the communication harder to monitor.

Dynamic Compression

I am very gratified to see Rappaport accept the use of dynamic compression:

> "To address Mr. Karn's question, I would support any data method, including documented dynamic compression, so long as it complied with FCC rules and came with a publicly available decoder that could be demonstrated to properly decode all transmissions by an eavesdropper, and was made widely available at little or no cost to the public for successful eavesdropping."

This resolves one of my primary objections, as dynamic compression is another way to improve communications efficiency with the side effect (intended or not) of making monitoring

more difficult. To reiterate, this is true even for a fully documented compression scheme with a publicly available decoder because of the “error propagating” nature of any efficient dynamic compression scheme. Rappaport now implicitly accepts that effective monitoring may require an error-free stream, which as discussed earlier cannot be guaranteed on a one-way radio channel even with FEC. And it implies acceptance of the principle that anything one might do to improve efficiency necessarily makes monitoring more difficult. This implicit contradiction undercuts almost all of Rappaport’s argument. His complaints can be resolved under the existing rules, and by the development of publicly available tools (both hardware and software) to monitor the Winlink network. For this reason, no changes to the rules are required.

I still respectfully request that the Commission dismiss RM-11831.

Respectfully submitted,

Philip R Karn Jr, KA9Q